

CYBER SECURITY

BLOCKCHAIN

CREATED BY :

PREM SHARMA

MCA(SE)

03716404520

What is BlockChain?

- Blockchain is a peer to peer transaction in a decentralized network establishing trust among unknown peers which records the transaction in an immutable distributed ledger.

Key characteristics of the blockchain architecture

- Cryptography** — Blockchain transactions are verified and trustworthy because of complex computations and cryptographic proof between the parties.
- Immutability** — Records in a blockchain can't be modified or deleted.
- Provenance** — It's possible to trace the origin of each transaction in the blockchain ledger.
- Decentralization** — Every member of the blockchain structure is able to access the entire distributed database. Unlike in a centralized system, a consensus algorithm is responsible for network management.
- Anonymity** — Every member of the blockchain network has a generated address, not a user ID. This preserves the anonymity of users, especially in a public blockchain.
- Transparency** — The blockchain system is unlikely to be damaged as it takes enormous computing power to completely rewrite the blockchain network.

Ethereum

- Ethereum is an open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology. Like Bitcoin, no one controls or owns Ethereum – it is an open-source project built by many people around the world. But unlike the Bitcoin protocol, Ethereum was designed to be adaptable and flexible. It is easy to create new applications on the Ethereum platform.
- Ethereum in the narrow sense refers to a suite of protocols that define a platform for decentralized applications. At the heart of it is the [Ethereum Virtual Machine \(“EVM”\)](#), which can execute code of arbitrary algorithmic complexity. In computer science terms, Ethereum is “Turing complete”. Developers can create applications that run on the EVM using friendly programming languages modelled on existing languages like JavaScript and Python.

Ganache

Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. You can use Ganache across the entire development cycle; enabling you to develop, deploy, and test your dApps in a safe and deterministic environment.

MetaMask

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

Tools Links

→ For Ganache:

◆ <https://trufflesuite.com/ganache/>

● For MetaMask:

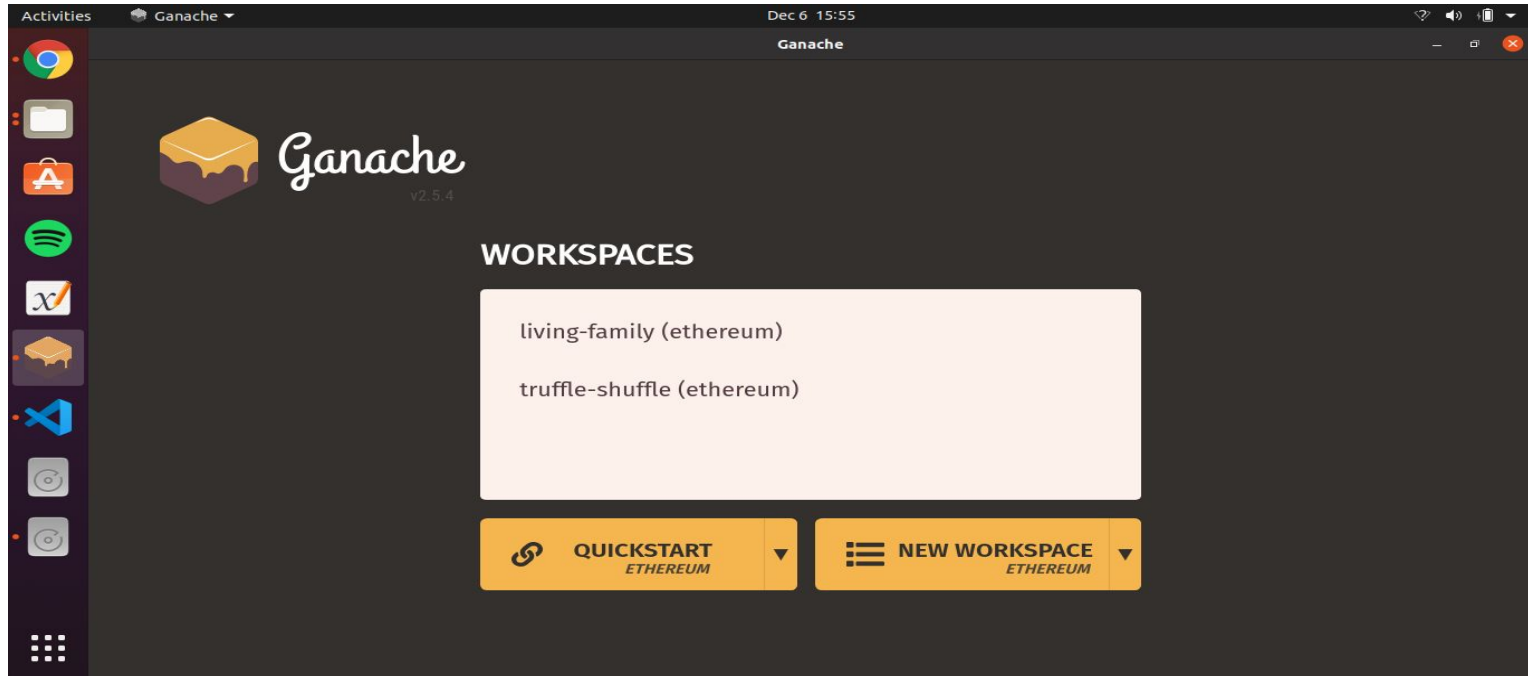
○ <https://metamask.io/>



TOOL DEMONSTRATION

Creating workspace

Local Blockchain using Ganache



ACCOUNTS

Local BlockChain on machine

Activities Ganache Dec 6 15:59

Ganache

ACCOUNTS BLOCKS TRANSACTIONS CONTRACTS EVENTS LOGS

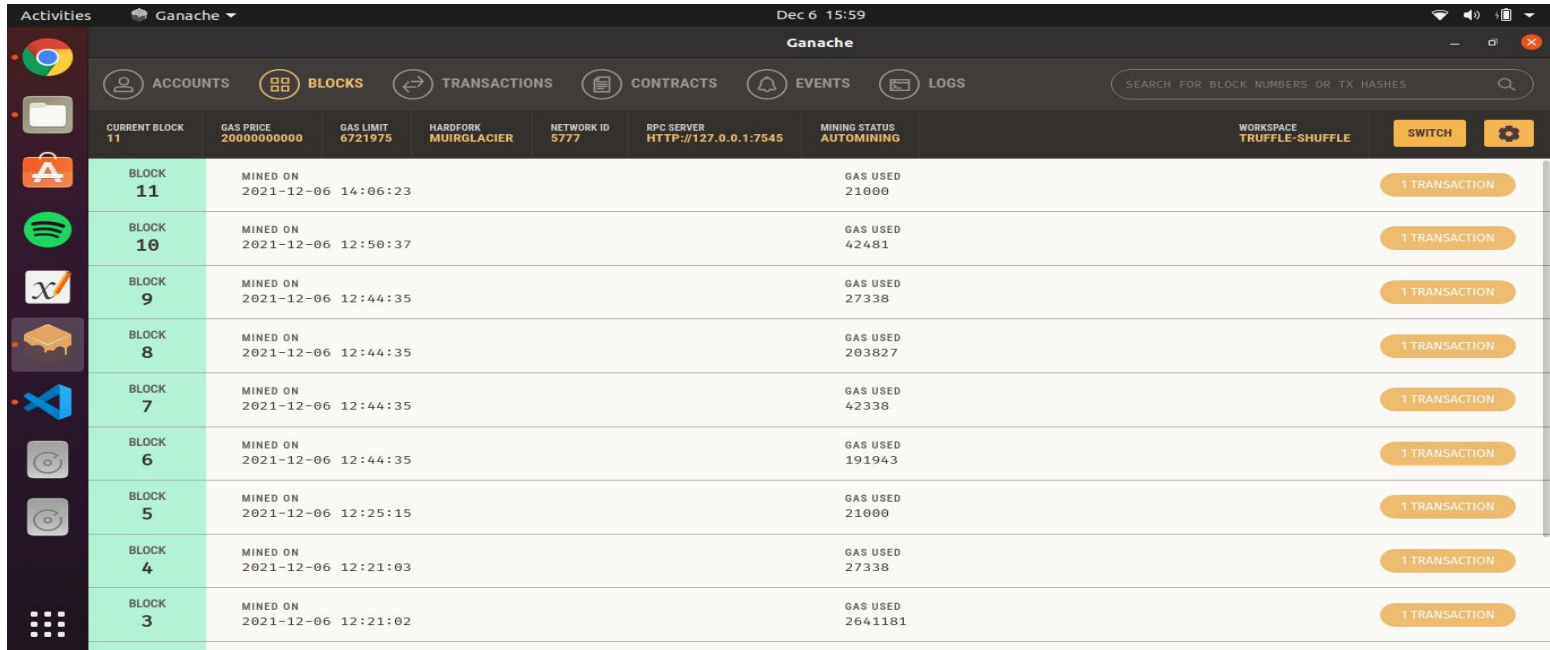
SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK 11 GAS PRICE 2000000000 GAS LIMIT 6721975 HARDFORK MUIRGLACIER NETWORK ID 5777 RPC SERVER HTTP://127.0.0.1:7545 MINING STATUS AUTOMINING WORKSPACE TRUFFLE-SHUFFLE SWITCH

MNEMONIC	HD PATH
dance infant spot antique title stock spider sweet online trial ski tree	m/44'/60'/0'/0/account_index
ADDRESS 0x21B24609251640230A9981bFf4E0dC7746b4776C	BALANCE 29.93 ETH TX COUNT 11 INDEX 0
ADDRESS 0xff5281c2084a3D5e45BCCdFfdc4aDA41aBcF0680	BALANCE 50.00 ETH TX COUNT 0 INDEX 1
ADDRESS 0xf90F12D2ecD8166dCFcb22bC7a6D1dA6B8B0a72A	BALANCE 50.00 ETH TX COUNT 0 INDEX 2
ADDRESS 0xc6882A1a686Cc1bcf712042716f991e8576e92ca	BALANCE 50.00 ETH TX COUNT 0 INDEX 3
ADDRESS 0x537Fd16f7F8fAD967440cE654185c381C96065bE	BALANCE 50.00 ETH TX COUNT 0 INDEX 4
ADDRESS 0x591CF5AECA925a9dcc9aaE62714730d2928A467b	BALANCE 50.00 ETH TX COUNT 0 INDEX 5

BLOCKS

Blocks in a BlockChain



The screenshot shows the Ganache desktop application interface. The top bar includes the title 'Ganache' and the date/time 'Dec 6 15:59'. Below the title bar is a navigation menu with icons for ACCOUNTS, BLOCKS (selected), TRANSACTIONS, CONTRACTS, EVENTS, and LOGS. A search bar on the right says 'SEARCH FOR BLOCK NUMBERS OR TX HASHES'. Below the navigation menu is a status bar with various metrics: CURRENT BLOCK 11, GAS PRICE 20000000000, GAS LIMIT 6721975, HARDFORK MUIRGLACIER, NETWORK ID 5777, RPC SERVER HTTP://127.0.0.1:7545, MINING STATUS AUTOMINING, and WORKSPACE TRUFFLE-SHUFFLE. There are also buttons for SWITCH and a settings gear icon. The main area displays a table of blocks, with columns for BLOCK number, MINED ON (timestamp), GAS USED, and a button for each transaction.

CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE	
11	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	TRUFFLE-SHUFFLE	<button>SWITCH</button> <button>⚙️</button>
BLOCK 11	MINED ON 2021-12-06 14:06:23		GAS USED 21000		<button>1 TRANSACTION</button>			
BLOCK 10	MINED ON 2021-12-06 12:50:37		GAS USED 42481		<button>1 TRANSACTION</button>			
BLOCK 9	MINED ON 2021-12-06 12:44:35		GAS USED 27338		<button>1 TRANSACTION</button>			
BLOCK 8	MINED ON 2021-12-06 12:44:35		GAS USED 203827		<button>1 TRANSACTION</button>			
BLOCK 7	MINED ON 2021-12-06 12:44:35		GAS USED 42338		<button>1 TRANSACTION</button>			
BLOCK 6	MINED ON 2021-12-06 12:44:35		GAS USED 191943		<button>1 TRANSACTION</button>			
BLOCK 5	MINED ON 2021-12-06 12:25:15		GAS USED 21000		<button>1 TRANSACTION</button>			
BLOCK 4	MINED ON 2021-12-06 12:21:03		GAS USED 27338		<button>1 TRANSACTION</button>			
BLOCK 3	MINED ON 2021-12-06 12:21:02		GAS USED 2641181		<button>1 TRANSACTION</button>			

TRANSACTIONS

Number of Transactions

Activities Ganache Dec 6 15:59

Ganache

ACCOUNTS BLOCKS **TRANSACTIONS** CONTRACTS EVENTS LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE	
11	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	TRUFFLE-SHUFFLE	SWITCH ⚙️

TX HASH
0xb0edf3a20493cf8d2788dc5c075579bf91afab657ef65a412240f41f63a7c4a9

FROM ADDRESS
0x21B24609251640230A9981bFf4E0dC7746b4776C

TO CONTRACT ADDRESS
0x394211b786C148A2683295Fdb23Cc1a4EaC09B47

GAS USED
21000

VALUE
10000000000000000000

CONTRACT CALL

TX HASH
0xc1f5c60b9abd151eed7b1cf26186d4d10ee04b7142a697aca6afb9c9665561a3

FROM ADDRESS
0x21B24609251640230A9981bFf4E0dC7746b4776C

TO CONTRACT ADDRESS
0x5142cA55478af45CCBF62dffE854E7f4A546ea4

GAS USED
42481

VALUE
0

CONTRACT CALL

TX HASH
0x4b9390b8a131f680c3b3e06f3e3241750c679b7543e1bec4eb07f53503c047d5

FROM ADDRESS
0x21B24609251640230A9981bFf4E0dC7746b4776C

TO CONTRACT ADDRESS
0x642338ED06C603FF842063aa47046072Dd7edc7

GAS USED
27338

VALUE
0

CONTRACT CALL

TX HASH
0x4cd5802b46c80413f54ecf5cc416806c3cd743ca6b39975330005e534d6c875a

FROM ADDRESS
0x21B24609251640230A9981bFf4E0dC7746b4776C

CREATED CONTRACT ADDRESS
0x5142cA55478af45CCBF62dffE854E7f4A546ea4

GAS USED
203827

VALUE
0

CONTRACT CREATION

INFORMATION IN A BLOCK

Block 11 with details

The screenshot shows the Ganache desktop application interface. The top bar includes the 'Activities' menu, the 'Ganache' logo, and the system clock 'Dec 6 15:59'. Below the top bar is a navigation menu with icons for ACCOUNTS, BLOCKS (highlighted), TRANSACTIONS, CONTRACTS, EVENTS, and LOGS. A search bar on the right says 'SEARCH FOR BLOCK NUMBERS OR TX HASHES'. Below the navigation menu is a status bar with various metrics: CURRENT BLOCK 11, GAS PRICE 2000000000, GAS LIMIT 6721975, HARDFORK MUIRGLACIER, NETWORK ID 5777, RPC SERVER HTTP://127.0.0.1:7545, MINING STATUS AUTOMINING, and WORKSPACE TRUFFLE-SHUFFLE. There are 'SWITCH' and 'SETTINGS' buttons on the right. The main content area is titled 'BLOCK 11' with a 'BACK' button. It displays the following information:

BLOCK 11	
GAS USED	21000
GAS LIMIT	6721975
MINED ON	2021-12-06 14:06:23
BLOCK HASH	0x1700c0bb8bdd629bc5ddf8f31b45b96c25dabb1c740807829470e3c952e5317
TX HASH 0xb0edf3a20493cf8d2788dc5c075579bf91afab657ef65a412240f41f63a7c4a9	
FROM ADDRESS 0x21824609251640230A9981bFf4E0dC7746b4776C	TO CONTRACT ADDRESS 0x394211b786C148A2683295FDb23Cc1a4EaC09B47
GAS USED	21000
VALUE	1000000000000000000

On the right side of the TX HASH section, there is a 'CONTRACT CALL' button. The left sidebar contains a vertical stack of application icons: Chrome, File Explorer, Brave, Spotify, X, a folder icon, Visual Studio Code, and two circular icons at the bottom.

INSIDE A TRANSACTION

Details of a transaction

The screenshot shows the Ganache desktop application interface. The top bar displays the time as 15:59 on Dec 6. The main navigation bar includes tabs for ACCOUNTS, BLOCKS, TRANSACTIONS (which is active), CONTRACTS, EVENTS, and LOGS. A search bar on the right of the navigation bar is labeled 'SEARCH FOR BLOCK NUMBERS OR TX HASHES'. Below the navigation bar, a status bar shows various network metrics: CURRENT BLOCK 11, GAS PRICE 20000000000, GAS LIMIT 6721975, HARDFORK MUIRGLACIER, NETWORK ID 5777, RPC SERVER HTTP://127.0.0.1:7545, MINING STATUS AUTOMINING, and WORKSPACE TRUFFLE-SHUFFLE. A 'SWITCH' button and a settings gear icon are also present.

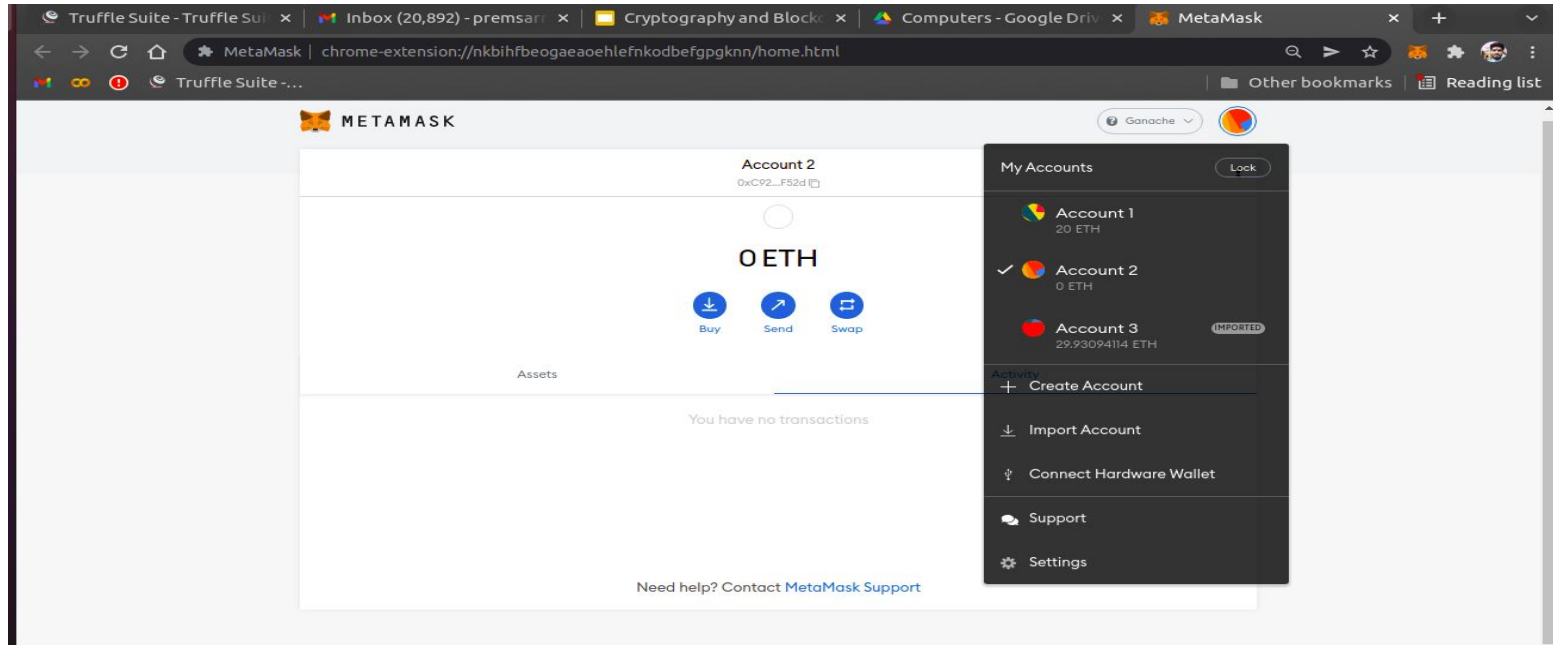
The main content area displays transaction details for TX 0xb0edf3a20493cf8d2788dc5c075579bf91afab657ef65a412240f41f63a7c4a9. A 'BACK' button is on the left. The transaction details are as follows:

SENDER ADDRESS		TO CONTRACT ADDRESS			
0x21B24609251640230A9981bFf4E0dC7746b4776C		0x394211b786C148A2683295FDb23Cc1a4EaC09B47		CONTRACT CALL	
VALUE	GAS USED	GAS PRICE	GAS LIMIT	MINED IN BLOCK	
10.00 ETH	21000	20000000000	21000	11	

Below the transaction details, there is a section for 'TX DATA' showing '0x'. Further down, an 'EVENTS' section is shown with the message 'NO EVENTS'.

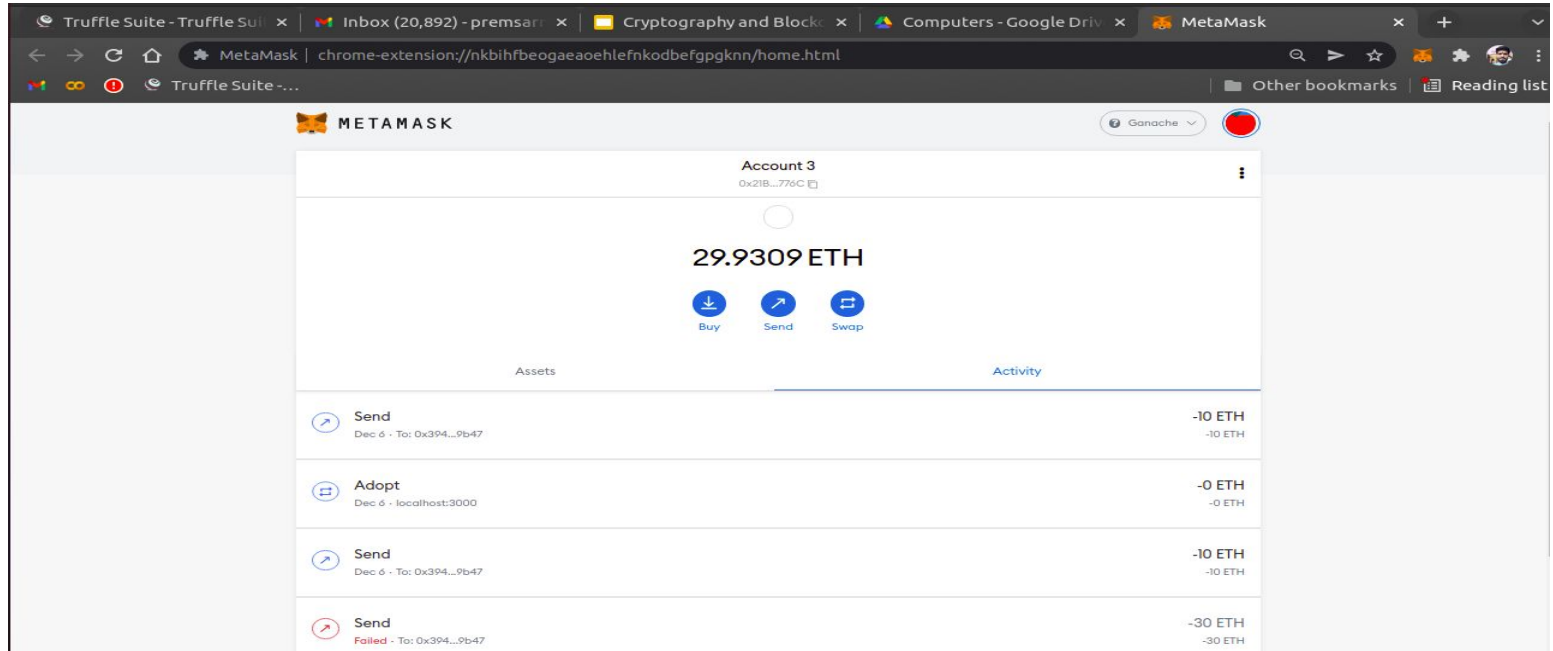
METAMASK

A Cryptocurrency wallet for Ethereum BlockChain



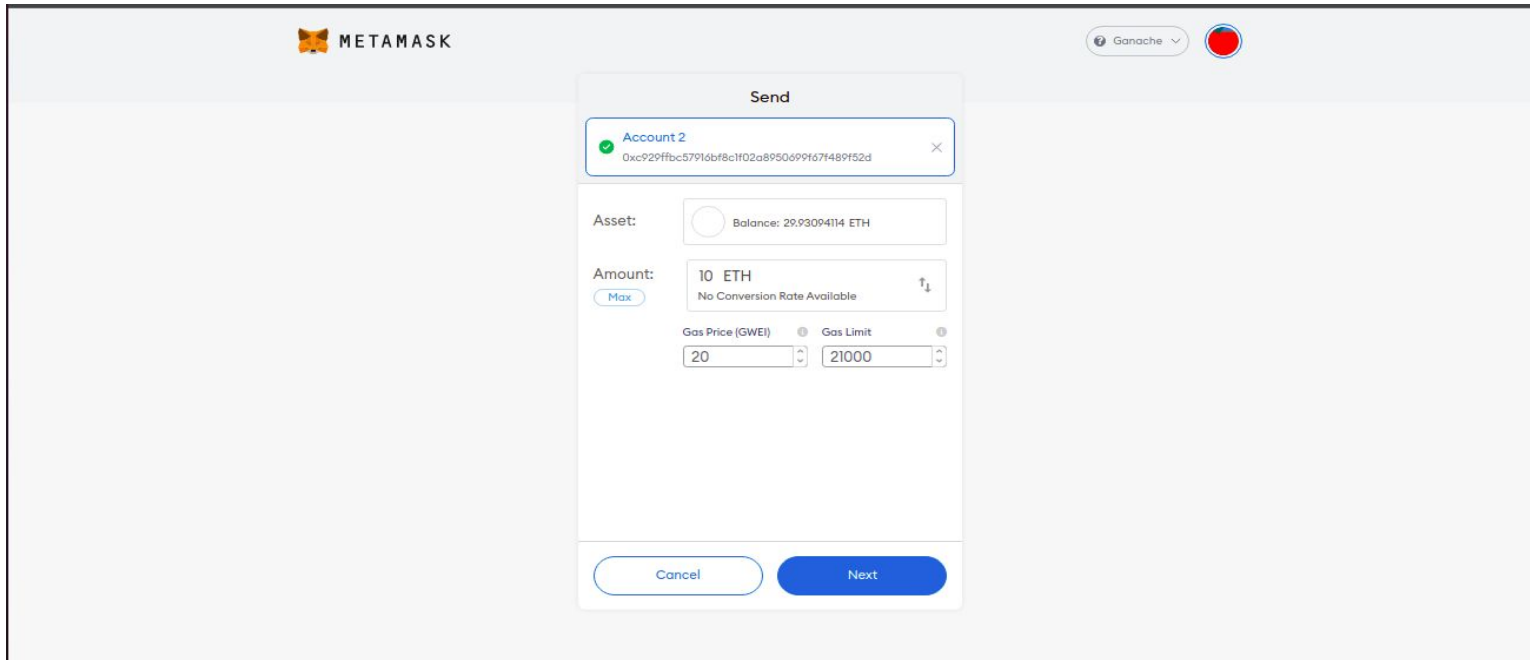
CONNECTING METAMASK

MetaMask Wallet connected with Ethereum Blockchain using Ganache



TRANSFERRING ETHER

Transferring ether to another account



The image shows the Metamask 'Send' transaction screen. At the top left is the Metamask logo. At the top right, there is a dropdown menu showing 'Ganache' and a red circular status indicator. The main content area is a modal titled 'Send'. Inside the modal, there is a recipient selection box at the top showing 'Account 2' with a green checkmark and a close button. Below this, the 'Asset' section shows a radio button selected for 'Balance: 29.93094114 ETH'. The 'Amount' section shows '10 ETH' with a 'Max' button and a conversion rate of 'No Conversion Rate Available'. Below the amount, there are two input fields: 'Gas Price (GWEI)' set to '20' and 'Gas Limit' set to '21000'. At the bottom of the modal are two buttons: 'Cancel' and 'Next'.

Send

Account 2
0xc929fbc57916bf8c1f02a8950699167f489f52d

Asset: ☐ Balance: 29.93094114 ETH

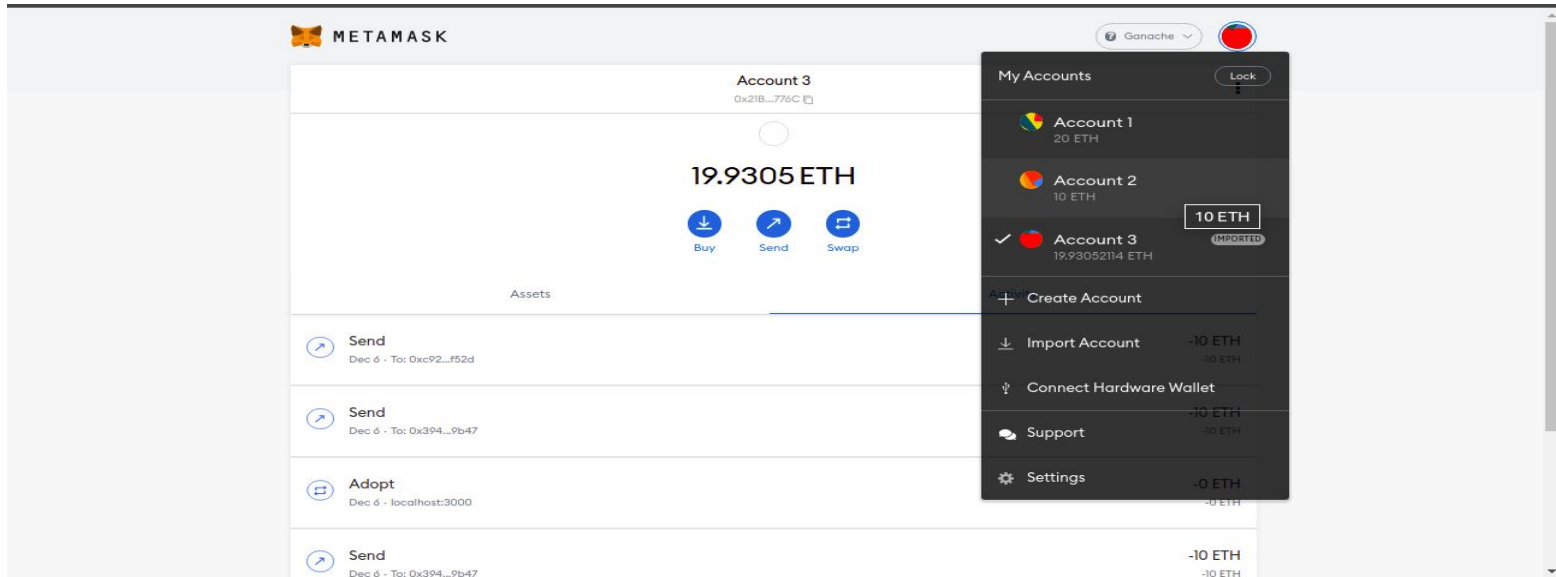
Amount: 10 ETH
No Conversion Rate Available

Gas Price (GWEI) 20 Gas Limit 21000

Cancel Next

Successful

Transaction of 10 ether is completed



Let's See it in Ganache

Block 12 For the transferring ether in metamask

Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
12

GAS PRICE
20000000000

GAS LIMIT
6721975

HARDFORK
MUIRGLACIER

NETWORK ID
5777

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

WORKSPACE
TRUFFLE-SHUFFLE

SWITCH

BACK

BLOCK 12

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
21000	6721975	2021-12-06 16:03:29	0xef334f4dd8a4db3cf98c2fd2c0a9d5cba65c52474159b34bd62d8dc0fd72cb5e

TX HASH

0x78f449af2ce0155678f70908a4e31e3cc6651cfcf41e17c7ba93c934b233f83b

CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0x21B24609251640230A9981bFf4E0dC7746b4776C	0xC929ffBC57916bf8c1F02A8950699f67F489F52d	21000	10000000000000000000

DEPLOY DAPP

Deploying Smart Contract over Ethereum BlockChain using truffle

```
prem@idwellin:~$ cd Desktop
prem@idwellin:~/Desktop$ cd pet-shop-tutorial
prem@idwellin:~/Desktop/pet-shop-tutorial$ truffle compile
```

```
Compiling your contracts...
=====
```

```
> Everything is up to date, there is nothing to compile.
```

```
prem@idwellin:~/Desktop/pet-shop-tutorial$ truffle migrate
```

```
Compiling your contracts...
=====
```

```
> Everything is up to date, there is nothing to compile.
```

```
EVENTS
```

```
NO EVENTS
```

```
Starting migrations...
```

```
=====
```

```
> Network name:      'development'
```

```
> Network id:        5777
```

```
> Block gas limit: 6721975 (0x6691b7)
```

CREATING BLOCK

Transaction completed for Dapp

[illegible]

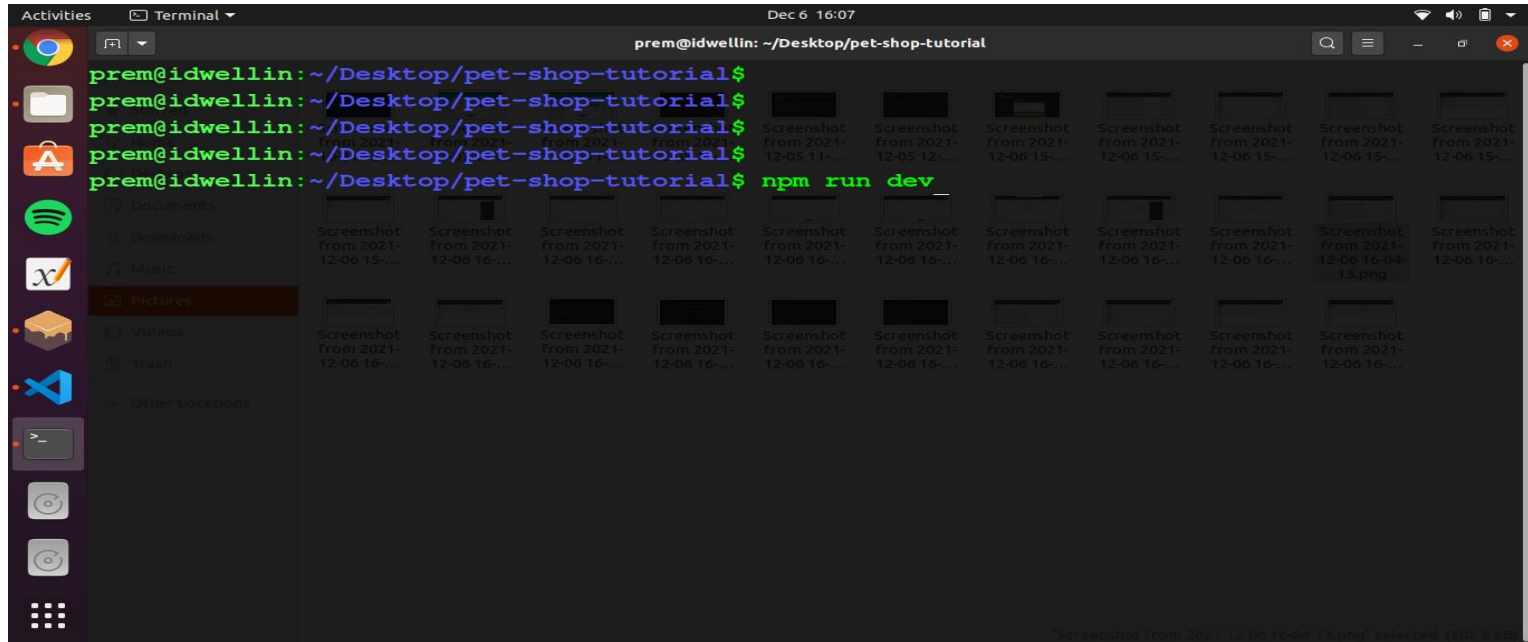
Transaction Completed

Blocks are added to the BlockChain

Ganache									
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS	SEARCH FOR BLOCK NUMBERS OR TX HASHES			
CURRENT BLOCK 16	GAS PRICE 20000000000	GAS LIMIT 6721975	HARDFORK MUIRGLACIER	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING	WORKSPACE TRUFFLE-SHUFFLE		SWITCH ⚙️
BLOCK 16	MINED ON 2021-12-06 16:05:54				GAS USED 27338		1 TRANSACTION		
BLOCK 15	MINED ON 2021-12-06 16:05:54				GAS USED 203827		1 TRANSACTION		
BLOCK 14	MINED ON 2021-12-06 16:05:54				GAS USED 42338		1 TRANSACTION		
BLOCK 13	MINED ON 2021-12-06 16:05:54				GAS USED 191943		1 TRANSACTION		
BLOCK 12	MINED ON 2021-12-06 16:03:29				GAS USED 21000		1 TRANSACTION		
BLOCK 11	MINED ON 2021-12-06 14:06:23				GAS USED 21000		1 TRANSACTION		
BLOCK 10	MINED ON 2021-12-06 12:50:37				GAS USED 42481		1 TRANSACTION		
BLOCK 9	MINED ON 2021-12-06 12:44:35				GAS USED 27338		1 TRANSACTION		
BLOCK 8	MINED ON 2021-12-06 12:44:35				GAS USED 203827		1 TRANSACTION		

Running Dapp

Using npm to run the app on local machine



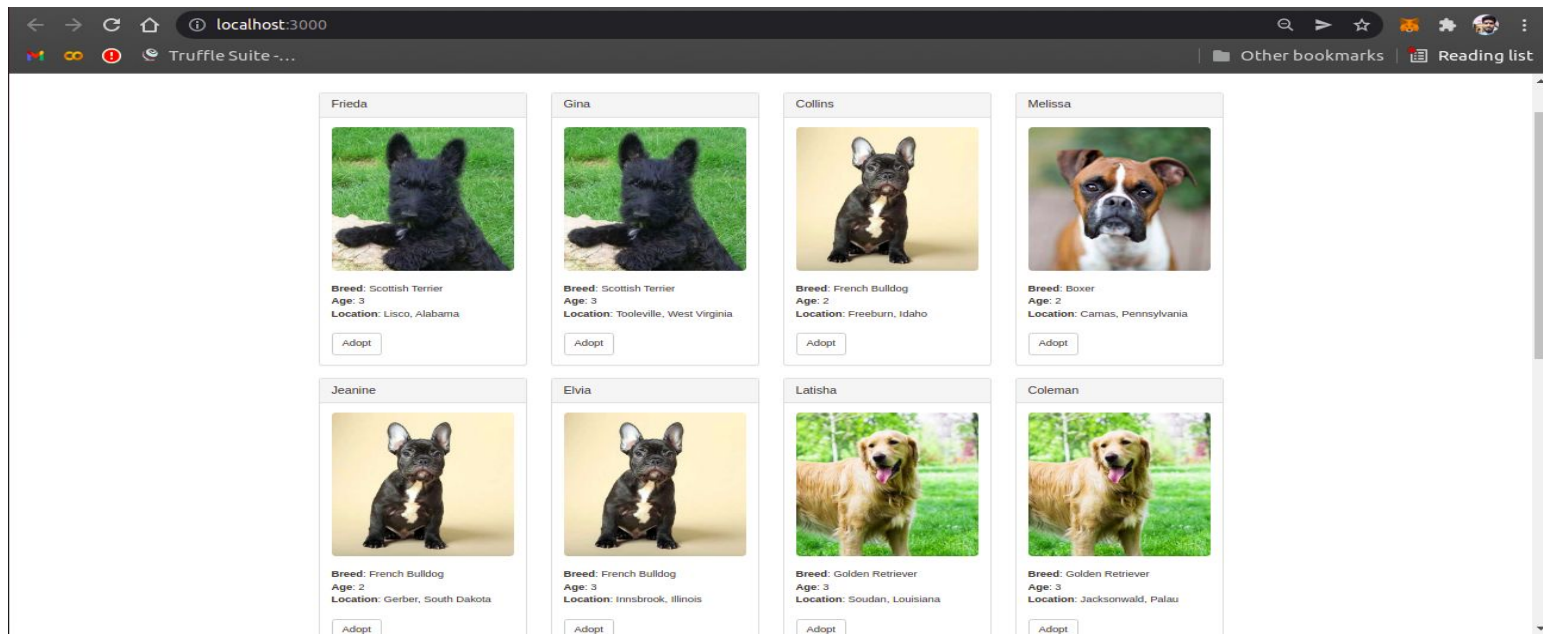
Fetching and Configuring

Processing.....

```
> lite-server
** browser-sync config **
{ injectChanges: false,
  files: [ './**/*.{html,htm,css,js}' ],
  watchOptions: { ignored: 'node_modules' },
  server:
    { baseDir: [ './src', './build/contracts' ],
      middleware: [ [Function], [Function] ] } }
[Browsersync] Access URLs:
-----
  Local: http://localhost:3000
  External: http://192.168.0.108:3000
-----
  UI: http://localhost:3001
  UI External: http://localhost:3001
-----
[Browsersync] Serving files from: ./src
[Browsersync] Serving files from: ./build/contracts
[Browsersync] Watching files...
```

THE DAPP CONTENT

Dogs Adoption using cryptocurrency




Dapp and MetaMask

Using MetaMask by connecting the Dapp

localhost:3000

Truffle Suite - ...


Frieda



Breed: Scottish Terrier
Age: 3
Location: Lisco, Alabama

Adopt


Gina



Breed: Scottish Terrier
Age: 3
Location: Tooleville, West Virginia

Adopt

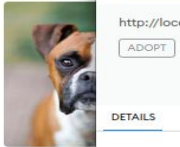
Collins



Breed: French Bulldog
Age: 2
Location: Freeburn, Idaho

Adopt


Melissa



Breed: Boxer
Age: 2
Location: Camas,

Adopt


Jeanine



Breed: French Bulldog
Age: 2
Location: Gerber, South Dakota

Adopt


Elvia



Breed: French Bulldog
Age: 3
Location: Innsbrook, Illinois

Adopt

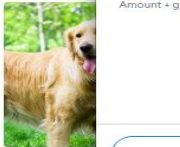
Latisha



Breed: Golden Retriever
Age: 3
Location: Soudan, Louisiana

Adopt

Coleman



Breed: Golden Retriever
Age: 3
Location: Jacksonwald, Palau

Adopt

Account 3

0x1c1...Db01

New address detected! Click here to add to your address book.

http://localhost:3000

ADOPT

DETAILS DATA

Estimated gas fee 0.00127406 0.001274 ETH

Max fee: 0.00127406 ETH

Total 0.00127406 0.00127406 ETH

Amount + gas fee Max amount: 0.00127406 ETH


Reject Confirm

Successful Transaction

Adoption is successful (see the first dog's success button)

localhost:3000 Truffle Suite ...


Frieda



Breed: Scottish Terrier
Age: 3
Location: Lisco, Alabama

Success

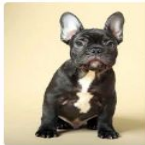
Gina



Breed: Scottish Terrier
Age: 3
Location: Tooleville, West Virginia

Adopt


Collins



Breed: French Bulldog
Age: 2
Location: Freeburn, Idaho

Adopt


Jeanine



Breed: French Bulldog
Age: 2
Location: Gerber, South Dakota

Adopt


Elvia



Breed: French Bulldog
Age: 3
Location: Innsbrook, Illinois

Adopt

Latisha



Breed: Golden Retriever
Age: 3
Location: Soudan, Louisiana

Adopt

Adopt

0x21B...776C → 0x1c1...Db01

Transaction

Nonce	16
Amount	-0 ETH
Gas Limit (Units)	63703
Gas Used (Units)	42469
Gas price	20
Total	0.00084938 ETH

Activity Log

- Transaction created with a value of 0 at 16:10 on 12/6/2021.
- Transaction submitted with estimated gas fee of 0 WEI at 16:10 on 12/6/2021.
- Transaction confirmed at 16:10 on 12/6/2021.

Let's see it in Ganache

Block 17 reflecting the txn of the same

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
17

GAS PRICE
20000000000

GAS LIMIT
6721975

HARDFORK
MUIRGLACIER

NETWORK ID
5777

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

WORKSPACE
TRUFFLE-SHUFFLE

SWITCH

BACK

BLOCK 17

GAS USED
42469

GAS LIMIT
6721975

MINED ON
2021-12-06 16:10:19

BLOCK HASH
0xb52b538ec824dc2f2e7d7fadc41aa97e4c8393a797178b3d597acfb3885f80c7

TX HASH
0x09ba26cbd1f4bbd6998c2e064d234c59749c46c76b45ad13f5e23c083c2824f0

CONTRACT CALL

FROM ADDRESS
0x21B24609251640230A9981bFf4E0dC7746b4776C

TO CONTRACT ADDRESS
0x1c14dC086AA226e576e9Df9997Bcd0AF6168Db01

GAS USED
42469

VALUE
0



Thank You